

IN THE UNITED STATES COURT
FOR THE DISTRICT OF PUERTO RICO

UNITED STATES OF AMERICA,

Plaintiff,

v.

MARÍA MILAGROS CHARBONIER-
LAUREANO [1], ORLANDO
MONTES-RIVERA [3], AND
ORLANDO GABRIEL MONTES-
CHARBONIER [4],

Defendants.

CRIM. No. 20-248 (SCC)

OMNIBUS OPINION AND ORDER

The Government seeks pretrial determinations on the admissibility and self-authentication of various public and private records. *See* Docket Nos. 411, 412. Defendant María M. Charbonier-Laureano (“Charbonier”) responds that the pretrial determinations sought are unnecessary. *See* Docket No. 459, pg. 1. Defendants Orlando Montes-Rivera and Orlando Gabriel Montes-Charbonier did not file responses. The Court addresses each motion in turn.

I. MOTION *IN LIMINE* AT DOCKET NO. 411

The Government asks this Court to declare that certain business and public records are (1) admissible non-hearsay under Federal Rule of Evidence 803(6) (“Records of a Regularly Conducted Activity”) and 803(8) (“Public Records”) and (2) self-authenticating under Rule 902(11) and 902(4). *See* Docket No. 411, pg. 1.

A. Admissibility

Out-of-court statements, when offered to prove the truth of the matter asserted, are hearsay and thus generally inadmissible. *See* FED. R. EVID. 801(c); FED. R. EVID. 802. But there are several exemptions, *see* FED. R. EVID. 801(d), and exceptions, *see* FED. R. EVID. 803; FED. R. EVID. 804(b); FED. R. EVID. 807. And, of course, if the out-of-court statements are being offered to prove something other than the truth of the matter asserted, they are not hearsay at all. *See United States v. Pena*, 24 F.4th 46, 61 (1st Cir. 2022).

The records at issue, if offered to prove the truth of the matter asserted, are hearsay. *See* FED. R. EVID. 801. While the

Government has identified potentially applicable exceptions to the rule against hearsay, other admissibility considerations remain. Accordingly, the Court declines to make a blanket ruling regarding these records' admissibility. Evidentiary rulings will be made at trial when the Court can examine the evidence offered.

B. Self-Authentication

Certain categories of evidence are self-authenticating and do not require extrinsic evidence, such as witness testimony, to support a finding that the evidence is what the proponent claims. *See* FED. R. EVID. 901, 902. Two such categories are certified copies of public records and certified domestic records of a regularly conducted activity. *See* FED. R. EVID. 902(4), (11).

The Government states they have obtained certifications compliant with Rule 902 for nearly all of the records described in its Motion at Docket No. 411. *See* Docket No. 411, pg. 7. The Government has not filed any certifications with the Court. Upon viewing the certifications, the Court

will determine whether they meet Rule 902's self-authentication criteria.

Accordingly, the Court **DENIES IN PART AND HOLDS IN ABEYANCE IN PART** the Motion at Docket No. 411 requesting a pretrial determination as to the admissibility and self-authentication of certain public and business records.

II. MOTION *IN LIMINE* AT DOCKET NO. 412

The Government also moves this Court for an order *in limine* declaring certain iCloud records produced by Apple, Inc. ("Apple") in response to search warrants as self-authenticating pursuant to Federal Rule of Evidence 902(11) ("Certified Domestic Records of a Regularly Conducted Activity").¹ See Docket No. 412, pg. 1; Docket No. 465, pg. 1.

¹ The Government initially argued Federal Rule of Evidence 902(14) ("Certified Data Copied from an Electronic Device, Storage Medium, or File") afforded a basis for finding the Apple iCloud reports self-authenticating. See Docket No. 412, pg. 1. The Government subsequently withdrew that argument. See Docket No. 465, pgs. 1–2. Because the Government did not argue the decryption and report generation processes yielded business records within the scope of Rule 902(11), the Court deems the Government's arguments as to those categories under Rule 902(14) withdrawn.

The Government provided corresponding certifications at Docket No. 454.

Rule 902(11) provides that:

The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record — and must make the record and certification available for inspection — so that the party has a fair opportunity to challenge them.

FED. R. EVID. 902(11). In turn, Rule 803(6) provides that:

A record of an act, event, condition, opinion, or diagnosis [is not excluded by the rule against hearsay] if:

(A) the record was made at or near the time by — or from information transmitted by — someone with knowledge;

(B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether

or not for profit;

(C) making the record was a regular practice of that activity[]

FED. R. EVID. 803(6)(A)–(C). “Rule 803(6) is designed to capture records that are likely accurate and reliable in content, as demonstrated by the trustworthiness of the underlying sources of information and the process by which and purposes for which that information is recorded.” *United States v. Browne*, 834 F.3d 403, 410 (3d Cir. 2016) (citing *E.C. Ernst, Inc. v. Koppers Co.*, 626 F.2d 324, 330–31 (3d Cir. 1980)). Classic examples of self-authenticating business records are bank and phone records. *See id.* at 436. The Court therefore must assess whether the certifications filed by the Government at Docket No. 454 meet the “requirements of Rule 803(6)(A)–(C), as shown by a certification of the custodian or another qualified person.” FED. R. EVID. 902(11).²

The Government cites no case law classifying iCloud

² The Rule 902(11) notice requirement appears met here by the Government’s motions at Docket Nos. 412, 454, and 465. No defendant has objected to the sufficiency of the notice given.

records as business records for self-authentication purposes under Rule 902(11). Nor does the Government analogize to routinely recognized business records like phone or bank records to demonstrate why iCloud records ought to qualify as such.

The certifications filed by the Government at Docket No. 454-1 assert that the author has authority to certify the records and recites modified language from Rule 803(6) in stating that the records were “made at or near the time by, or from information transmitted by, someone with knowledge or from a process or system that produces an accurate result, the accuracy of which is regularly verified by Apple.”³ Docket

³ The certification appears to conflate Rules 901 and 902. Rule 901(b)(9) permits authentication through “[e]vidence describing a process or system and showing that it produces an accurate result.” This authentication method requires extrinsic evidence, whereas self-authenticating evidence need not be accompanied by extrinsic evidence. In essence, the certification states in the disjunctive that the records either meet the criteria for a self-authenticating business record *or* were produced by a process or system that produces an accurate result. No extrinsic evidence as to the reliability of that system was provided. The Court will not declare these records authentic on such unstable ground.

No. 454-1, pg. 2. The certification does not, however, include any information regarding the process or system by which Apple generated the records or the author's knowledge of the same.⁴ *See id.* Absent case law and developed arguments, the Court is not yet convinced that iCloud records qualify as self-authenticating business records.

In sum, the Government has not met their burden to demonstrate the records produced pursuant to the search warrant served on Apple are self-authenticating under Rule 902(11). Accordingly, the Court **DENIES WITHOUT PREJUDICE** the Motion at Docket No. 412 to the extent that it asks this Court to deem self-authenticating the records produced by Apple in response to search warrants.⁵ The

⁴ Some courts consider the certification author's knowledge of the process by which records are kept and generated in assessing the certification's sufficiency. *See* Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 7145, n. 20–21 (2021).

⁵ The Court makes no ruling as to whether media or communications derived from the iCloud accounts are attributable to the iCloud account owners of record. The Government will need to demonstrate that link at trial. The Court will rule on the admissibility of the iCloud records

Government only argued self-authentication was proper under Rule 902(14) regarding the Federal Bureau of Investigation's decryption and digital identification processes and the Cybercrime and Intellectual Property Section Laboratory's generation of "Cellebrite" reports in its Motion at Docket No. 412. Because the Government subsequently withdrew all arguments made under Rule 902(14), the Court **DEEMS WITHDRAWN** all arguments as to the iCloud records in those processing phases.

III. CONCLUSION

For the reasons above, the Court **DENIES IN PART AND HOLDS IN ABEYANCE IN PART** the Motion at Docket No. 411. The Court further **DENIES WITHOUT PREJUDICE** the Motion at Docket No. 412 with regard to the records produced by Apple pursuant to search warrants and **DEEMS WITHDRAWN** all arguments related to self-authentication under Rule 902(14).

produced by Apple and any reports generated from those records at trial.

The Parties shall inform if they agree to stipulate as to the authenticity of any records during the discussion of housekeeping matters on the first day of trial.

IT IS SO ORDERED.

In San Juan, Puerto Rico, this 5th day of December 2023.

S/ SILVIA CARREÑO-COLL

UNITED STATES DISTRICT COURT JUDGE